

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of	:	
	:	
Yung-Cheng LEE et al.	:	Group Art Unit: Not Yet Assigned
	:	
Application No.: Not Yet Assigned	:	Examiner: Not Yet Assigned
	:	
Filed: August 26, 2003	:	
	:	
For: HIGH-SECURITY ENCODING DEVICE FOR REMOTE CONTROLLER		

CLAIM TO PRIORITY UNDER 35 U.S.C. § 119

Assistant Commissioner of Patents
Washington, D.C. 20231

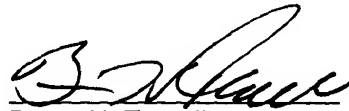
Sir:

Pursuant to the provisions of 35 U.S.C. § 119 and 37 C.F.R. § 1.55, Applicant claims the right of priority based upon **Taiwanese Application No. 091119738 filed August 30, 2002.**

A certified copy of Applicant's priority document is submitted herewith.

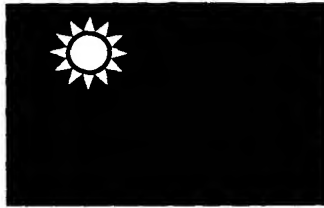
Respectfully submitted,

By:


Bruce H. Troxell
Reg. No. 26,592

TROXELL LAW OFFICE PLLC
5205 Leesburg Pike, Suite 1404
Falls Church, Virginia 22041
Telephone: (703) 575-2711
Telefax: (703) 575-2707

Date: August 26, 2003



中華民國經濟部智慧財產局

INTELLECTUAL PROPERTY OFFICE
MINISTRY OF ECONOMIC AFFAIRS
REPUBLIC OF CHINA

茲證明所附文件，係本局存檔中原申請案的副本，正確無訛，
其申請資料如下：

This is to certify that annexed is a true copy from the records of this
office of the application as originally filed which is identified hereunder：

申 請 日：西元 2002 年 08 月 30 日
Application Date

申 請 案 號：091119738
Application No.

申 請 人：盛群半導體股份有限公司
Applicant(s)

局 長

Director General

蔡 練 生

發文日期：西元 2002 年 9 月 30 日
Issue Date

發文字號：09111019053
Serial No.

申請日期	
案 號	
類 別	

A4
C4

(以上各欄由本局填註)

發 明 專 利 說 明 書		
一、發明 名稱	中 文	高安全性之遙控器編碼裝置
	英 文	
二、發明 創作人	姓 名	李永振、吳佳儒
	國 籍	中華民國
	住、居所	雲林縣虎尾鎮文化路 64 號 雲林縣斗六市大學路 3 段 123 號
三、申請人	姓 名 (名稱)	盛群半導體股份有限公司
	國 籍	中華民國
	住、居所 (事務所)	新竹市科學工業園區研新二路三號
	代 表 人 姓 名	吳啟勇

經濟部智慧財產局員工消費合作社印製

裝

訂

線

本紙張尺度適用中國國家標準 (CNS) A4規格 (210×297公釐)

四、中文發明摘要（發明之名稱：

高安全性之遙控器編碼裝置

本發明揭露一種高安全性之遙控器編碼裝置，包括：一計時器，以提供一發射計時值；一模式選擇器，以提供一模式選擇值；一控制器，接收一認證序號、該發射計時值與該模式選擇值，以產生一控制訊號；一密鑰；一加密器，係接收該控制訊號，並且以該密鑰將該控制訊號加密成密文；以及一射頻調變器，係將該密文調變並且將之輸出。本發明更揭露一種改善遙控器耗電之方法，包括：啟動編碼裝置；啟動編碼裝置之計時器；將該計時器之發射計時值與認證序號加密，並將之傳送至該解碼裝置；解碼裝置將所接收之資料與本身之計時值進行比對；解碼裝置之計時器與編碼裝置之計時器同步；判斷在一段時間內，是否有再次啟動編碼裝置；若否，則計時停止，但最後之計時值仍儲存於記憶體中，若是，則重複以上步驟，直到所控制之裝置被啟動。

英文發明摘要（發明之名稱：

（請先閱讀背面之注意事項再填寫本頁各欄）

裝

訂

線

五、發明說明(1)

(一) 發明領域：

本發明係有關一種遙控器編碼裝置，尤其是一種高安全性之遙控器編碼裝置，其特徵在於以計時器來取代習知技藝中的計數器，使得「阻擋—重送」攻擊難以得逞，以提高遙控系統之安全性，並且改善遙控器之耗電問題。

(二) 相關技藝的說明：

遙控器已儼然成為人們日常生活用品之一，舉凡汽車、家戶大門甚或視聽器材等，均需透過無線遙控以方便使用。雖然若干遙控對象不需有防止他人誤用、竊用等安全機制，但亦有甚多之應用需以安全為首要考慮。如汽車遙控器等應防止竊賊侵入偷竊汽車，甚至視聽器材亦需有若干安全之設計，以避免小孩觀看兒童不宜之節目等。

一般而言，遙控系統可分為單向操作與雙向操作等方式。在單向操作系統中，控制訊號全由發射端發射，以遙控接收端之設備；而雙向操作系統之控制訊號係經由發射端與接收端交互運作，以確定控制之目的。雙向操作系統雖然可達到雙方確認性(mutual authentication)，且可獲得較佳之控制效果，但因設備較複雜與昂貴，故除若干重要場合外甚少使用。

最簡單之遙控系統，係將控制訊號直接以明文(plaintext)用無線方式傳送至接收器。若每次傳送之明文均相同，則攻擊者利用掃描器截獲(eavesdrop)訊號後，只要將訊號重送(replay)即可攻擊成功，因此系統極不安全。即使系統傳送

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明 (8)

之訊號包括亂數與時間等非固定數值，若攻擊者獲悉系統架構與運作方式（通常可輕易獲得），可偽造一有效之訊號，亦可成功地攻擊系統。

較安全之方式，係將控制訊號適當地加密（encrypt）後始予送出，接收端收到訊號解密（decrypt）後再執行。此方式若採用安全之加密器，攻擊者無法獲悉控制訊號之正確內容。然而，若此係統如上述一樣，每次傳送之資料均相同，則攻擊者截獲訊號後，只要將訊號重送亦必可攻擊成功，即系統仍極不安全。但若系統傳送之訊號非固定，而是由若干亂數（random number）或碼簿（codebook）產生，只要亂數或碼簿之熵（entropy）夠大，即使攻擊者知悉系統架構與運作方式，因缺乏正確之密鑰，無法偽造有效之資料，故無法成功地攻擊系統。但由於下列因素，使傳統遙控器安全堪虞：

- 一、傳統遙控器之亂數個數或碼簿大小；
- 二、傳統遙控器系統架構與運作方式不安全。

上述因素致使攻擊者可輕易地猜出訊號內容，或經由錄下之全部控制訊號，再依序送出以啟動接收器。因此傳統之遙控系統，無論控制訊號加密與否，均易受攻擊。

欲使遙控系統達到安全之需求，必須使用現代密碼技術始能達成。加解密系統分為對稱金鑰加解密系統（symmetric key crypto-system）與非對稱金鑰加解密系統（asymmetric key crypto-system）等二種。分述如下：

- 一、對稱金鑰加解密系統：對稱金鑰加解密系統又稱傳統加解密系統，如圖1A所示。在圖1A中，系統之發射端的加

（請先閱讀背面之注意事項再填寫本頁）

裝
訂
線

五、發明說明 (3)

密金鑰1與接收端之解密金鑰2完全相同。在操作時，加密器3首先以密鑰1將明文M加密成密文C (ciphertext)。接收端在收到此密文C後，解密器4以相同於金鑰1之密鑰2解密成為明文M。根據美國國家標準之資料加密標準 (data encryption standard, DES)，輸入端之明文M係以64位元為單位切割成為多個區塊，將各區塊以64位元之密鑰加密成為64位元之密文C；接收端再以相同之密鑰K解密成為64位元之明文M。由於明文與密文長度相同，傳輸上較為經濟。

二、非對稱金鑰加解密系統：非對稱金鑰加解密系統又稱為公開金鑰 (Public key) 加解密系統，如圖1B所示。在圖1A中，系統之發射端的加密金鑰1'與接收端之解密金鑰2'並不相同。以著名的Rivest-Shamir-Adelman (RSA) 加密系統為例，輸入明文M以接收端之公開金鑰1'加密成為密文C，即 $C=M^e \pmod{N}$ 。接收端收到後再以己方之秘密金鑰 (Private key) 2'解密回復為明文M，即 $M=C^d \pmod{N}$ 。其中N為系統之公開值，係為二大質數p與q之相乘積，且 $e \cdot d = 1 \pmod{\phi(N)}$ 。非對稱金鑰加密系統中為達安全起見，通常N之數值均相當大 (至少1024位元長度)，且因採用指數運算，使得計算時間相當冗長，因此較難用單晶片等方式實現；而通常以軟體方式配合具高速運算之電腦來完成。不過因非對稱金鑰加密系統具有認證之功能，在網路與電子商業等應用上不可或缺。

針對目前最常使用的遙控系統，如美國專利案號5,517,187所揭露之遙控系統，其中該系統之發射器與接收器

五、發明說明(4)

的示意圖係分別如圖2A與圖2B所示。在圖2A中，發射器10包括：一計數器11，以提供一發射計數值 C_T ；一模式選擇器12，以提供一模式選擇值 M_o ；一控制器13，接收該發射計數值與該模式選擇值，以產生一控制訊號，其係以明文 M 表示；一密鑰14；一加密器15，係接收該控制訊號，並且以該密鑰14將該控制訊號加密成密文 C ；以及一射頻調變器16，係將該密文調變並且將之輸出。而在圖2B中，接收器20包括：一射頻解調器16'，以將發射器所輸出的訊號將以解調；一密鑰14；一解密器15'，係接收該解調訊號，並且以該密鑰14將該解調訊號解密成明文 M ；一計數器11，以產生一接收計數值 C_R ；一控制器13，接收該明文與該接收計數值；以及一檢查器17，檢查計數器之值是否正確以決定是否繼續執行。

其中，發射器之控制訊號 M 包括該模式選擇值 M_o 與該發射計數值 C_T ，即：

$$M=\{M_o, C_T\}$$

其中 M_o 為模式選擇暫存器之值，長度為32bits，其內容為模式選擇按鍵資訊、公司產品編號、其他相關與預備之保留位元等。模式選擇可分為正常或同步模式，其傳送資料與接收檢查步驟相似，僅檢查之資料位元與範圍不同而已。 C_T 為存放計數器之值，因計數器總長度為32bits，故其密碼共計 2^{32} 個。對於一般之遙控器而言，其安全度應已足夠。

系統中發射與接收端均具一共同之密鑰 K ，且各有一32位元之計數器。系統開始運作或重整後，接收端計數器 C_R 之

五、發明說明(5)

內容為發射端計數器 C_T 加1。發射端之計數器每次發射前計數器 C_T 之值即加一。發射端將上述資料M用K以對稱金鑰之方式加密後，傳送至接收端。

綜言之，美國專利案號5,517,187所揭露之遙控系統的操作方法，其特徵在於該接收端收到發射端的輸出訊號後，檢查：

一、決定係為正常或同步模式；

二、決定接收到的發射計數值 C_T 與接收端計數器之值 C_R 是否相符，即 $n \geq C_T - C_R \geq 0$ ；其中， n 為與安全有關之係數。例如取 $n=5$ ，即允許系統發射器最多五次發射失敗；

三、上述步驟二若符合，則使計數器同步（即令 $C_R = C_T + 1$ ），並啟動開關；若不符則不動作。此時若發射端傳送同步要求之訊號，系統即進入同步模式，執行後接收端計數器將與發射端同步且正常動作。（其程序與正常之步驟相同，惟傳送之資料改為另一組密碼與計數值，同時將安全係數放大，如取 $n=100$ 等）；以及

四、若正常模式或同步模式均無法啟動接收器，即應送回重新燒錄或檢修。

然而，此系統有一重大之缺失，即系統在傳送訊號時，若攻擊者將此訊號阻擋（mask），使接收端20無法正常收到訊號，此時接收端將無動作。一般使用者若使用遙控器數次而接收器20無法正常工作時，通常會離開請求支援。但此時攻擊者5若將接收之訊號重送給接收端20，只要計數器之數值在合理之範圍內，接收器20即會正常運作，亦即攻擊會得逞。

五、發明說明 (6)

使用同步模式時，仍如前述，攻擊亦會成功。由於無線遙控訊號之開放性，且攻擊者很容易購得任何型式之掃描器，故違法者可輕易地截獲並記錄任何訊號，經過接收阻擋、訊號截獲再訊號重送（簡稱「阻擋—重送」），攻擊即可輕易得逞，如圖3所示。

此外，尚有一種滾碼式（rolling code）系統以及一種跳頻式（hopping code）系統。在滾碼式系統中，接收器每收到一次訊號，無論訊號正確與否，計數器會立即加上一數值，例如1。因而在每一次的正常操作中，若攻擊者截獲訊號後再重送給接收者，則因接收器之計數器值大於訊號者，故無法正常運作。例如原本發射器之計數值為100而接收器值為101，此時發射器若發射訊號，則其計數值變為101；當接收器收到正確之訊號時，因兩計數值之資料相符，系統即正常運作，並將計數器加1而使其值成為102。若某攻擊者側錄獲取該計數值內容為101之傳送訊號，再重送此訊號給接收端，此時因接收端之計數器已為102，故資料不相符，使得系統停止運作。但若攻擊者不斷地重複送出此訊號，系統接收端雖不致於正常輸出，但由於接收端之計數值因不斷累加而超出安全範圍，致使系統從此無法運作，必須送回製造商處重新設定。

是以，在滾碼式系統中，若攻擊者使用如上述之方法將訊號阻擋，由於接收端之計數器保持原值，此時攻擊者若將截獲之訊號重送，接收器即會正常運作，使得攻擊得逞。

另外，跳頻式系統亦如上所述，唯其計數器為跳躍式之

（請先閱讀背面之注意事項再填寫本頁）

裝

訂

線

五、發明說明(7)

輸出(亦即,可經由虛擬亂數產生器達成),亦難以抵擋「阻擋一重送」式的攻擊。

因此,如何針對上述習用技藝的缺點而提出一種高安全性遙控器編碼裝置,除了可以成功抵禦「阻擋一重送」式的攻擊之外,更可以改善遙控器之耗電問題,即為本發明之發明重點。

(三) 發明之簡要說明:

基於解決以上所述習知技藝的缺失,本發明之主要目的在於提供一種高安全性遙控器編碼裝置,其使用一計時器,可成功地抵禦「阻擋一重送」式的攻擊,以提高系統之安全性。

為了達到本發明之上述目的,本發明揭露一種高安全性遙控器編碼裝置,包括:一計時器,以提供一發射計時值;一模式選擇器,以提供一模式選擇值;一控制器,接收一認證序號、該發射計時值與該模式選擇值,以產生一控制訊號;一密鑰;一加密器,係接收該控制訊號,並且以該密鑰將該控制訊號加密成密文;以及一射頻調變器,係將該密文調變並且將之輸出。

該計時器長度可依設計需要而有不同,一般係可選用8位元、16位元或32位元之計時器。

較佳者,該密鑰係為一64位元密鑰,亦可依需要增加或縮短位元數,例如16、32、128位元等。

較佳者,該密鑰係存放於一非揮發性(non-volatile)記

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明(8)

憶體中或使用一次可程式唯讀記憶體(one time program ROM)。

該發射計時值之長度依選用的計時器而定，如32位元計時器則計時值長度為4個位元組(byte)，其用來檢查編碼裝置的計時器與對應之解碼裝置的計時器之間的時間差是否在一容忍時間內。

較佳者，該模式選擇值之長度為2個位元組，用以根據實際需要從正常模式、緊急模式與同步模式中選擇一種模式。

較佳者，該認證序號之長度為2個位元組，供對應之解碼裝置驗證用。

較佳者，該控制訊號係以明文M表示。

較佳者，該密文係以對稱金鑰方式加密者。

較佳者，該計時器係以單晶片中之計時中斷方式實現之。

較佳者，該計時器係以一邏輯電路實現之。

本發明更揭露一種改善遙控器耗電之方法，包括：啟動編碼裝置；啟動編碼裝置之計時器；將該計時器之發射計時值與認證序號加密，並將之傳送至該解碼裝置；解碼裝置將所接收之資料與本身之計時值進行比對；解碼裝置之計時器與編碼裝置之計時器同步；判斷在一段時間內，是否有再次啟動編碼裝置；若否，則計時停止，但最後之計時值仍儲存於記憶體中，若是，則重複以上步驟，直到所控制之裝置被啟動。

為進一步對本發明有更深入的說明，乃藉由以下圖示、圖號說明及發明詳細說明，冀能對 貴審查委員於審查工作

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明(9)

有所助益。

(四) 圖式之簡要說明：

圖1A係為習用之對稱金鑰加密系統的方塊示意圖；

圖1B係為習用之非對稱金鑰加密系統的方塊示意圖；

圖2A係為美國專利案號5,517,187之遙控系統的發射器之方塊示意圖；

圖2B係為美國專利案號5,517,187之遙控系統的接收器之方塊示意圖；

圖3係為習用遙控系統之「阻擋—重送」的攻擊方式的方塊示意圖；

圖4A係為本發明具體實施例之遙控器編碼裝置之方塊示意圖；

圖4B係為本發明具體實施例之遙控器解碼裝置之方塊示意圖；

圖5係為本發明具體實施例之計時器之方塊示意圖；

圖6係為本發明另一具體實施例之計時器之方塊示意圖；以及

圖7係為本發明解碼裝置容忍時間(Tolerance time)、安全時間(Safe time)、計時晶片準確度(Accuracy)和啟動時間間隔之關係。

圖號對照說明：

1 加密金鑰

2 解密金鑰

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明(1°)

3	加密器	4	解密器
1'	加密金鑰	2'	解密金鑰
3'	加密器	4'	解密器
10	發射器	20	接收器
11	計數器	12	模式選擇器
13	控制器	14	密鑰
15	加密器	16	射頻調變器
15'	解密器	16'	射頻解調器
17	檢查器		
30	編碼裝置	40	解碼裝置
31	計時器	31'	計時器
32	模式選擇器		
33	控制器	33'	控制器
34	密鑰	34'	密鑰
35	加密器	36	射頻調變器
35'	解密器	36'	射頻解調器
37	暫存器		
51	震盪器	52	分頻器
53	單晶片內建計數器	54	系統計數器
61	震盪器	62	分頻器
63	計數器		

(五) 本發明之詳細描述：

本發明揭露一種高安全性之遙控器編碼裝置，其特徵在

(請先閱讀背面之注意事項再填寫本頁)

裝
訂
線

五、發明說明(11)

於以計時器來取代習知技藝中的計數器，使得「阻擋—重送」攻擊難以得逞，以提高遙控系統之安全性，並且改善遙控器之耗電問題。其詳細說明係參照以下之圖式來使之更為明白，其中相同的參考數字表示相同之元件。

煩請參閱圖4A，其係為本發明具體實施例之遙控器編碼裝置之方塊示意圖。在圖4A中，該編碼裝置30包括：一計時器31，以提供一發射計時值 T_T ；一模式選擇器32，以提供一模式選擇值 M_o ；一控制器33，接收一認證序號 N 、該發射計時值與該模式選擇值，以產生一控制訊號；一密鑰34；一加密器35，係接收該控制訊號，並且以該密鑰34將該控制訊號加密成密文 C ；以及一射頻調變器16，係將該密文調變並且將之輸出。

詳而言之，在本發明的編碼裝置中，該計時器係為一32位元計時器而且該密鑰係為一64位元密鑰。該密鑰係存放於一非揮發性(non-volatile)記憶體如ROM或EPROM中。

該控制訊號係以明文 M 表示為： $M=\{M_o, N, T_T\}$ 。其中， M_o 為模式選擇(mode select)值， N 為認證序號(identity)， T_T 為發射計時值，係分別說明如下：

一、 M_o ：模式選擇，長度為2個位元組，其包括模式選擇以及其他備用資料，用以根據實際需要從正常模式、緊急模式與同步模式中選擇一種模式。

1) 正常模式：使用於正常使用時。在本模式中，相對應之解碼裝置的容忍時間(tolerant time, T_L)較小。容忍時間係保證系統能正常運作時，解碼裝置所設定之編碼與解

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明 (12)

碼裝置的兩計時器的最大誤差值。容忍時間比一般安全時間 (safe time) 大。安全時間則為編碼與解碼裝置的兩計時器的實際最大誤差值。例如，若計時器的準確度為 $\pm 10 \cdot 10^{-6}$ 時，編碼與解碼裝置的兩計時器的實際最大誤差值即為 $20 \cdot 10^{-6}$ ，約為2sec/天。相當於30天的安全時間為1分鐘。若取容忍時間為安全時間的兩倍，則表示容許編碼與解碼裝置的兩計時器之間的誤差值為2分鐘。如此可保證系統可以正常運作，不致因系統計時誤差因故增加，而無法啟動之困擾。

2) 緊急模式：如果編碼與解碼裝置雙方因故計時誤差超過正常模式之容忍時間，則正常模式將無法啟動裝置。此時可利用緊急模式解決。此模式運作如正常模式，唯解碼裝置之容忍時間較大。但此模式系統安全度將降低，啟動裝置後應注意不可在容忍時間內離開。

3) 同步模式：若正常模式與緊急模式皆無法使解碼裝置輸出動作，則進入同步模式。此模式於解碼裝置端之檢查內容更為寬鬆，例如只比對認證序號或容忍時間等。此方法如前述緊急模式一般，系統安全度更低，應更注意在容忍時間內攻擊者「阻擋—重送」之問題。

二、N：認證序號，長度為2個位元組，供對應之解碼裝置驗證用，且其內容包括產品序號或其他參數。

三、 T_T ：發射計時值，長度為4個位元組 (byte)，其用來檢查編碼裝置的計時器與對應之解碼裝置的計時器之間的時間差是否在一容忍時間內。

此外，該控制訊號係以明文M表示。而且該密文係以對

五、發明說明 (13)

稱金鑰方式加密者，且其長度為64位元。

為配合本發明具體實施例之遙控器編碼裝置，其對應之解碼裝置40，如圖4B所示，係可包括：一射頻解調器36'，以將編碼裝置所輸出的訊號將以解調；一密鑰34'；一解密器35'，係接收該解調訊號，並且以該密鑰34'將該解調訊號解密成明文M；一計時器31'，以產生一接收計時值 T_R ；一控制器33'，接收該明文與該接收計數值；以及一暫存器37。

請注意，編碼裝置30與解碼裝置40之密鑰34、34'之內容相同。其中，在進行解碼運作時，控制器33'從M中取出 M_0 、N與 T_T ，再執行下列程序。

- 1) 判斷N是否正確，若否則停止輸出。
- 2) 若N無誤，判別此訊號為正常模式，緊急模式抑或同步模式。
- 3) 比較 T_T 與 T_R 是否在容忍時間內，即比對是否 $|T_T - T_R| \leq T_L$ 。若是則正常啟動輸出，否則系統即停止運作。唯在同步模式時，接收端只檢查認證序號，或如上述方式仍檢查容忍時間，但此容忍時間 T_L 之設定值更大，更易啟動輸出設備。（三種模式解碼裝置之檢查內容，可依系統需要設計調整）。
- 4) 無論正常模式、緊急模式或同步模式，解碼裝置確認輸入無誤後，即啟動輸出設備，並紀錄 T_T 以供爾後檢查訊號是否重送。
- 5) 重設計時訊號 T_R 使其與接收之計時訊號 T_T 同步，即令 $T_R = T_T$ ，以免爾後產生累計誤差。

（請先閱讀背面之注意事項再填寫本頁）

裝

訂

線

五、發明說明(14)

若正常模式、緊急模式或同步模式均無法啟動解碼裝置時，即表示編碼裝置與解碼裝置雙方計時器之間的差值甚大，或裝置故障，即應送回重新設定或檢修。

在本發明中，計時器可由單晶片之計時中斷方式為之，或另設置一計時裝置達成。亦即若編碼裝置以成本因素、電路複雜度電力消耗為考慮，而僅以邏輯電路完成者，可用一簡單之計時電路實現。解碼裝置因較不用考慮上述因素，通常均設置一單晶片，故可擇中斷方式計時或另置計時電路為之。計時器並不需如一般計時裝置如手錶等，需達到和現在時間同步與解析度達到毫秒甚至微秒之效果，而是僅為一簡單之計時裝置，其解析度達到0.5秒即可。且為達保密之效果，計時器之初值可以亂數為之，亦即起始值不為零，使攻擊者甚難猜中計時值。

為保證系統安全與正常運作，計時器應達輸出不易重複以及編碼裝置與解碼裝置之兩計時器雙方同步之要求。

以盛群半導體所研發之單晶片HT48C50為例，若採用400KHz振盪器，且16位元計時器設定為0.5Sec中斷一次，產生 2^{32} 次中斷之時間約為24855天。亦即若計時輸出至4個暫存器，則循環一次約需68年，故計時訊號不虞發生重複現象。以單晶片計時中斷與計時邏輯電路實現之計時器方塊分別如圖5與圖6所示。在圖5中，計時器係以單晶片中之計時中斷方式實現之，該計時器包括：一震盪器51、一分頻器52、一單晶片內建計數器53、以及一系統計數器54。在圖6中，計時器係以邏輯電路實現之，其包括：一震盪器61、一分頻器62、

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明 (15)

以及一計數器63。

在編碼裝置與解碼裝置之兩計時器的同步方面，以現今計時器之穩定度約 $\pm 10 \cdot 10^{-6}$ 計算，約69天始產生1分鐘之誤差；收發二方產生之最大差值為 $20 \cdot 10^{-6}$ ，亦即約為2sec/day。若設定容忍時間為1分鐘，則在34天內應不虞發生收發雙方不同步之情形。為避免收發二方因計時之誤差而產生解碼裝置無法運作之窘況，系統應以軟體程式適當調整容忍時間 T_L 。容忍時間 T_L 之設計可如下式：

$$T_L = \alpha \cdot T_S + C$$

$$T_S = T_d \cdot A_c$$

其中 α ：為一常數，此值可視需要調整之。例如在正常模式時可設定為1~2，在緊急模式時可定為3~5，在同步模式時可設定為5以上。

T_d ：為兩次啟動之相隔時間 (time-between-operations)。

T_S ：安全時間，為收發二方之計時器之最大誤差時間。

C ：時間常數。利用此時間常收以保證系統能正常運作。上述公式若無此參數 C ，則當兩次連續按鍵時，因 T_d 甚小成 $T_L \approx 0$ 。故當第二次按鍵時，因收發二方計時進位之時間差，可能致使解碼裝置無法運作。 C 值通常取0.5秒即可。

A_c ：收發雙方計時之準確度之相加值。

例如若系統收發雙方之計時裝置準確度為 $\pm 10 \cdot 10^{-6}$ ，則

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明 (16)

$Ac=20 \cdot 10^{-6}$ ，收發雙方最大之計時差值約為2sec/day。若此次運作距上次成功操作之時間為10天，則 $T_s=T_d \cdot Ac=10\text{days} \cdot 20 \cdot 10^{-6}=17.28\text{sec}$ 。若 $\alpha=1.5$ 且 $C=0.5\text{sec}$ ，則容忍時間 $T_L=\alpha \cdot T_s+C=1.5 \cdot 17.28\text{sec}+0.5\text{sec}=26.42\text{sec}$ ，即發射者若發射失敗，只要在26.5秒後始離開，攻擊者即無法利用阻擋—重送方法啟動解碼裝置。

圖7說明解碼裝置容忍時間 T_L (Tolerance time)、安全時間 T_s (Safe time)、計時晶片準確度 Ac (Accuracy) 和啟動時間間隔之關係。

若攻擊者將訊號阻擋，使接收端無法收到訊號，則接收端將無動作。一般使用者若無法啟動裝置時，通常會在現場揣摩一段時間再離開。若經容忍時間 T_L 後，攻擊者將接收之訊號重送給接收端，由於接收端計時值已超過 T_L ，解碼裝置即拒絕正常動作，因此攻擊不會得逞。若攻擊者仍不斷地嘗試重送，則需24855天計時始回到原來之值，故攻擊者甚難利用重送來侵入系統。此種「阻擋—重送」攻擊又可分為下列二種情形：

1) 系統已久未運作，即 $T_d \gg 0$ ，致使容忍時間增大，使用者需於較長之時間後始能離開（如前述，若此次運作距上次成功操作之時間為10天，則應停留26.5秒後始能離開），以確保系統安全。否則若攻擊者進行阻擋—重送攻擊，因容忍時間較大之故，攻擊可能會得逞。

2) 系統剛完成一次成功的運作後，使用者緊接著再一次執行，但攻擊者此時進行阻擋—重送攻擊，致使合法使用者

（請先閱讀背面之注意事項再填寫本頁）

裝 · 訂 · 線

五、發明說明(17)

無法正常執行此次運作。此時因系統 $T_d \approx 0$ ，縱使此使用者立刻離開，攻擊者亦無法啟動輸出，攻擊不會成功。

解碼裝置有數組暫存器存放使用過之 T_T ，故若攻擊者截獲一次正常運作之訊號而立刻重送時，系統可偵測攻擊者之重複訊號而予拒絕。且當攻擊者等待一段時間後再重送時，系統因已超過容忍時間，亦可檢查出攻擊者而停止輸出。

由於每次執行解碼裝置之計時均重整與編碼裝置之時間相同，且以軟體控制容忍時間隨啟動之時間間隔適當調整，故無累計誤差且不虞同步問題。

系統採用安全之加密器如DES等，攻擊者欲猜中收發雙方之密鑰 K ，需時 $2^{56} \mu s$ （設攻擊者之電腦能在1秒內執行百萬次之猜測），即約需2285年。且因系統未送出相關之明文，攻擊者缺乏明文與密文進行比對，甚難求出正確的密鑰。

系統軟硬極為簡單，其複雜度如同目前市售產品，並未增加過多電路與運算。本發明與美國專利案號5,517,187所揭露之遙控系統之比較係如表一所示：

（請先閱讀背面之注意事項再填寫本頁）

裝

訂

線

五、發明說明(18)

表一、本發明與美國專利案號5,517,187之遙控系統之比較

系 統 項 目	本發明	美國專利案號 5,517,187
關鍵技術	計時器32位元	計數器32位元
密鑰長度	64位元	64位元
能抵擋「重送」攻擊	是 但需多出數組32bit 暫存器以存用過的 T _T 值	是 但如不斷重送則可 攻擊成功
能抵擋「阻擋—重 送」攻擊	是 但當多時未用，需 於較長之容忍時間 後始能離開	不能

以下，在本發明中，亦揭露一種改善遙控器耗電問題之方法，藉以延長電池的使用壽命。

本發明之遙控系統之編碼裝置與解碼裝置皆設有計時器，且二者均存有加密器如DES等與加解密金鑰K。計時器一旦啟動後即不斷計時，對於接收端的解碼裝置而言，通常因為裝設的地點而能接在固定電源設備，如汽車電瓶或家用電源，較無省電的考量，但是發射端的編碼裝置因為一般係手持設備使用電池為電源，故會有省電或換電池的考量。在省電考量情況下，仍可運用本發明之手段加以操作，以下提出兩種省電的實施方式：

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明(19)

第一種方式為：除了前述加解密的方式外，對於計時值的比對可改為差值比較，即在發射端每次操作時才啟動計時器一段時間，雖然該計時值與接收端的計時值可能不同，但基於設計時採用相同計時頻率的元素，兩個計時器的計時速度相同，所以接收端的解碼裝置可以比對該計時值的計時速度而確認發射端是否為配對之編碼裝置。換言之，發射端開始操作後，計時器開始運作，並不斷送出改變的計時值，接收端即判斷該計值的計時頻率是否與接收端相同而決定是否為配對之遙控器。

第二種方式為：當發射端一段時間不使用時，其計時器即停止計時工作，直到使用者再次按下發射端的遙控器按鍵時，計時器才繼續計時，因為此情況下發射端與接收端的計時器的值必不相同，所以必須使首次發送出去的訊號為強制同步模式的訊號，接收端接收到該強制同步模式訊號時，即可讓接收端的計時器與發射端的計時器同步，因此發射端下一個發送出去的訊號便可依前述正常的方式進行判斷。由於僅在發射端計時器停止後的首次發射訊號為強制同步模式訊號，其長度約僅有數毫秒左右的時間，所以使用者一般並不會有延遲的感覺，因為發射完強制同步模式訊號後接著即會送出正常的訊號，或者要求使用者在一段時間不用遙控器時需連按兩次發射按鍵，接收端才會動作，第一次是送出強制同步訊號，第二次才是正常訊號。為了安全性考量，防止有心者在旁截錄強制同步模式訊號及後續正常訊號，可以進一步使接收端記錄前幾次強制同步模式時的計時值，如果與記

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明 (20)

錄相同表示為攻擊者的複製訊號，即不會有開啟的動作。

上述改善遙控器耗電之方法，可以表示為，包括：啟動編碼裝置；啟動編碼裝置之計時器；將該計時器之發射計時值與認證序號加密，並將之傳送至該解碼裝置；解碼裝置將所接收之資料與本身之計時值進行比對；若在強制模式下，解碼裝置之計時器將與編碼裝置之計時器同步；若在一般模式下，解碼裝置將依接收之計時值判斷是否啟動編碼裝置；為省電考量，編碼裝置之控制器將判斷在某一時間內是否有按鍵，若無按鍵即啟動省電裝置自行斷電；無論何種模式，發射器最後之計時值仍將儲存於其記憶體中。一般而言，當解碼裝置收到第一次訊號時，因時間差值甚大應無法真正啟動所控制之裝置。但經計時器同步後，第二次之訊號應可使系統啟動該裝置。

由於一般編碼裝置中之單晶片或其他電子裝置，其計算能力有限，無法快速完成非對稱系統所需的模乘法(modular multiplication)或模指數(modular exponentiation)等較複雜之運算，故宜採用對稱式之加解密器實現。以目前仍公認安全之DES系統為例，單晶片利用對稱式方法執行一次加密或解密所需之時間，約僅需數毫秒，使用上應無時間延遲過久之問題。雖然新公佈的加密標準AES即將取代使用二十年之久的DES，本發明亦可將系統之加密器改為AES，唯因AES之密鑰較長，加解密之時間將稍長。

綜上所述，本發明揭露一種高安全性之遙控器編碼裝置，其特徵在於以計時器來取代習知技藝中的計數器，使得

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明 (✓)

「阻擋一重送」攻擊難以得逞，以提高遙控系統之安全性，並且改善遙控器之耗電問題。因此，本發明案在目的及功效上均深富實施之進步性，極具產業之利用價值，且為目前市面上前所未見之運用，依專利法之精神所述，本發明案完全符合發明專利之要件。

唯以上所述者，僅為本發明之較佳實施例而已，當不能以之限定本發明所實施之範圍，即大凡依本發明申請專利範圍所作之均等變化與修飾，皆應仍屬於本發明專利涵蓋之範圍內，謹請 貴審查委員明鑑，並祈惠准，是所至禱。

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

六、申請專利範圍

1. 一種高安全性遙控器編碼裝置，係包括有：
 - 一計時器，以提供一發射計時值；
 - 一模式選擇器，以提供一模式選擇值；
 - 一控制器，接收一認證序號、該發射計時值與該模式選擇值，以產生一控制訊號；
 - 一密鑰；一加密器，係接收該控制訊號，並且以該密鑰將該控制訊號加密成密文；以及
 - 一射頻調變器，係將該密文調變並且將之輸出。
2. 如申請專利範圍第1項所述之高安全性遙控器編碼裝置，其中該計時器係為一32位元計時器。
3. 如申請專利範圍第1項所述之高安全性遙控器編碼裝置，其中該密鑰係為一64位元密鑰。
4. 如申請專利範圍第3項所述之高安全性遙控器編碼裝置，其中該密鑰係存放於一非揮發性(non-volatile)記憶體中。
5. 如申請專利範圍第1項所述之高安全性遙控器編碼裝置，其中該發射計時值之長度為4個位元組(byte)，其用來檢查編碼裝置的計時器與對應之解碼裝置的計時器之間的時間差是否在一容忍時間內。
6. 如申請專利範圍第1項所述之高安全性遙控器編碼裝置，其中該模式選擇值之長度為2個位元組，用以根據實際需要從正常模式、緊急模式與同步模式中選擇一種模式。
7. 如申請專利範圍第1項所述之高安全性遙控器編碼裝置，其中該認證序號之長度為2個位元組，供對應之解碼裝置

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

六、申請專利範圍

驗證用。

8. 如申請專利範圍第1項所述之高安全性遙控器編碼裝置，其中該控制訊號係以明文表示。
9. 如申請專利範圍第1項所述之高安全性遙控器編碼裝置，其中該密文係以對稱金鑰方式加密者，且其長度為64位元。
10. 如申請專利範圍第1項所述之高安全性遙控器編碼裝置，其中該計時器之初值係為亂數。
11. 如申請專利範圍第10項所述之高安全性遙控器編碼裝置，其中該計時器係以一邏輯電路實現之。
12. 如申請專利範圍第10項所述之高安全性遙控器編碼裝置，其中該計時器係以單晶片中之計時中斷方式實現之。
13. 一種高安全性遙控器編碼裝置，係包括有：
 - 一計時器，以提供一發射計時值，該計時器僅在遙控器編碼裝置被操作時才計時數秒以節省電能；
 - 一模式選擇器，以提供一模式選擇值；
 - 一控制器，接收一認證序號、該發射計時值與該模式選擇值，以產生一控制訊號；
 - 一密鑰；一加密器，係接收該控制訊號，並且以該密鑰將該控制訊號加密成密文；以及
 - 一射頻調變器，係將該密文調變並且將之輸出。
14. 如申請專利範圍第13項所述之一種高安全性遙控器編碼裝置，其操作方法係包括有：
 - 啟動編碼裝置；

(請先閱讀背面之注意事項再填寫本頁)

裝
訂
線

六、申請專利範圍

啟動編碼裝置之計時器；

將該計時器之發射計時值與認證序號及強制同步模式值加密，並將之傳送至外部的解碼裝置，使該解碼裝置的計時器進行同步動作；

判斷在一段時間內，是否有再次啟動編碼裝置；

若否，則計時停止，但最後之計時值仍儲存於記憶體中，若是，則送出不含強制同步模式值的加密訊號。

(請先閱讀背面之注意事項再填寫本頁)

裝
訂
線

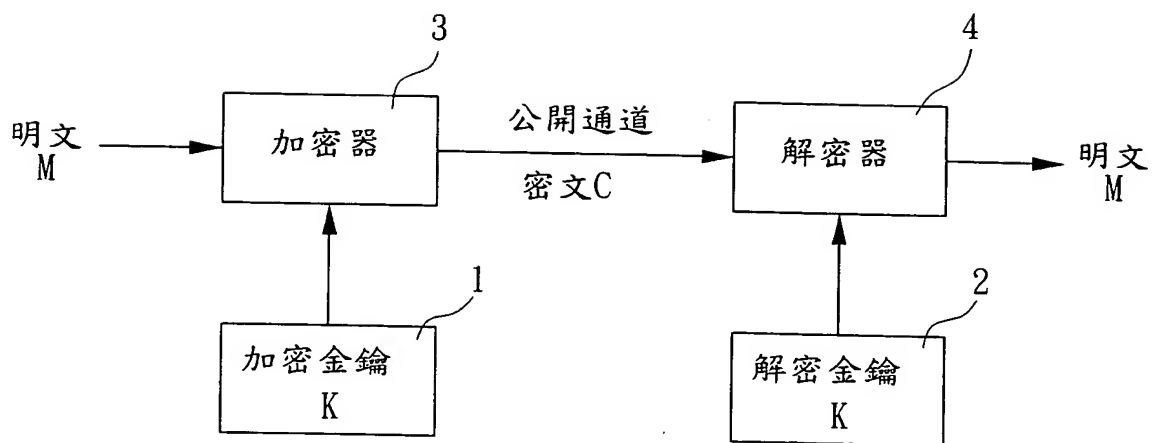


圖 1 A
(習用技術)

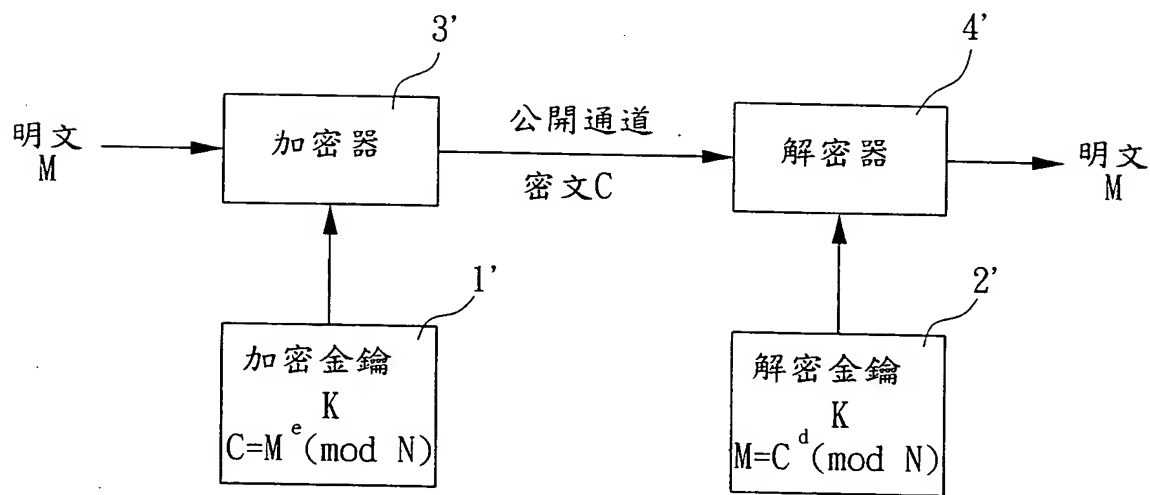


圖 1 B
(習用技術)

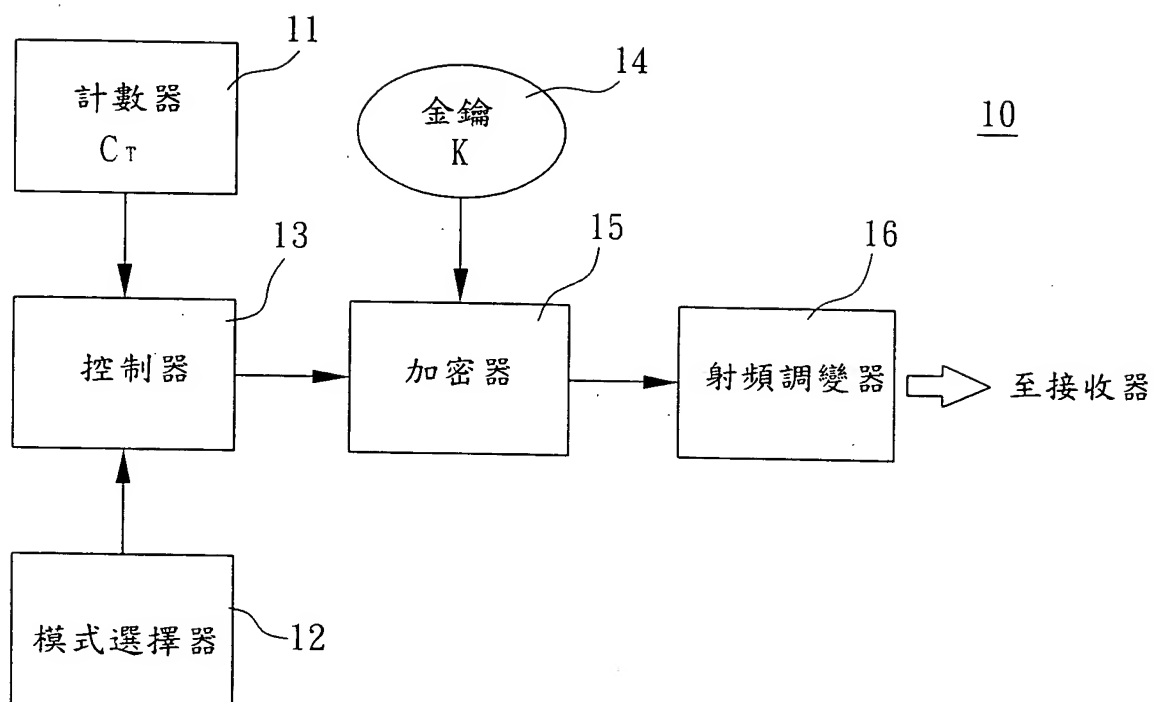


圖 2 A
(習用技術)

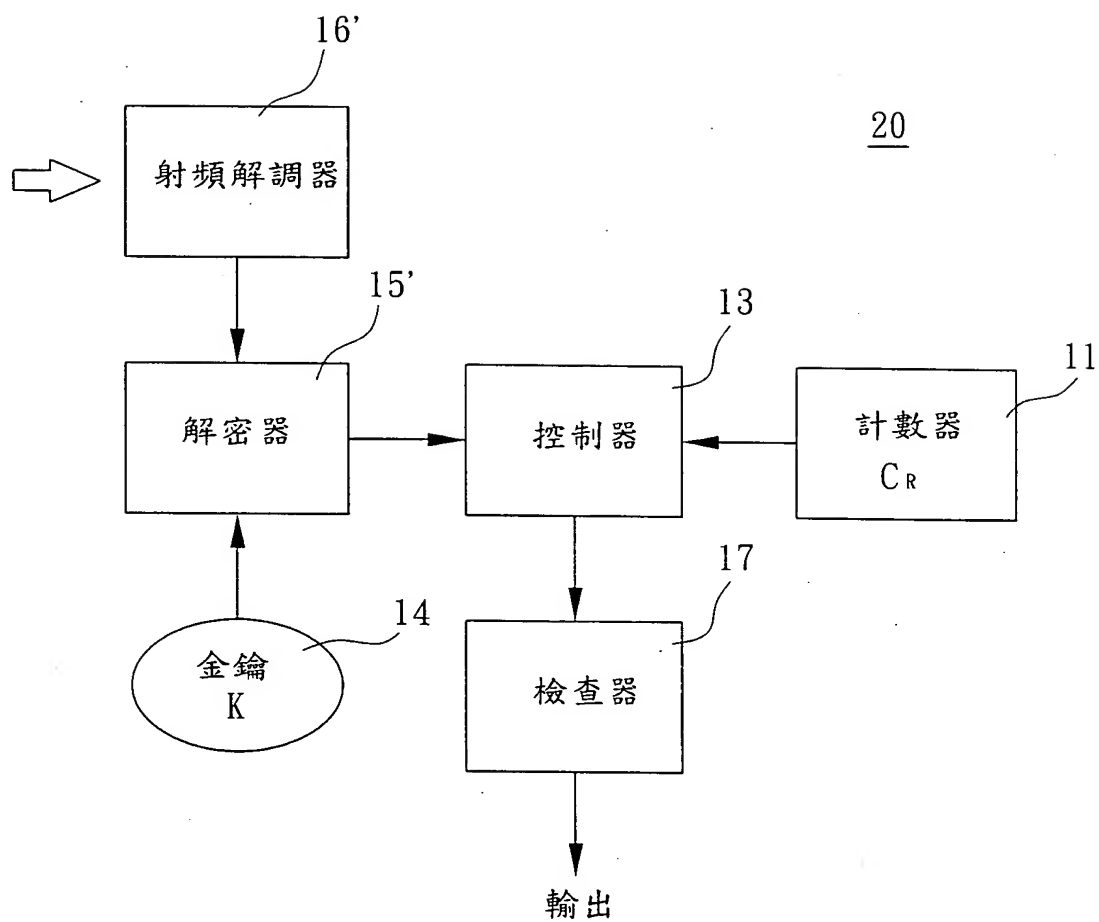


圖 2 B
(習用技術)

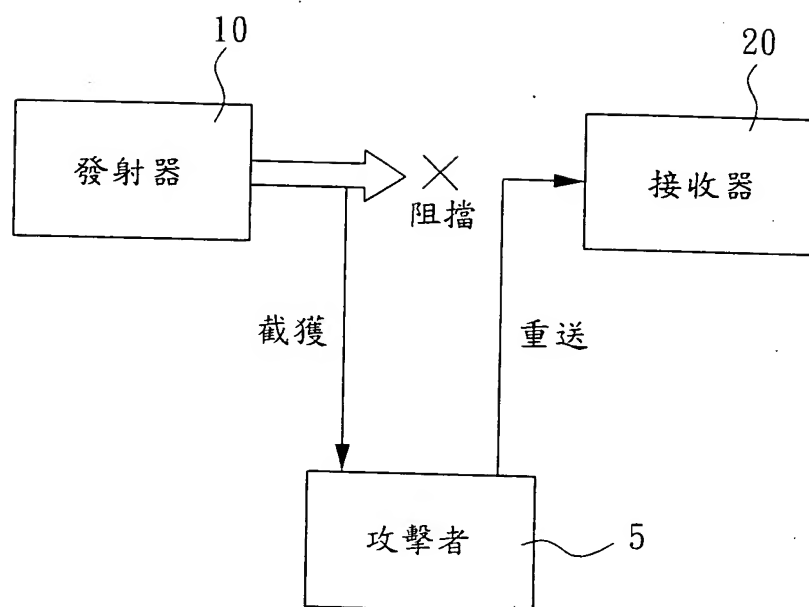


圖 3
(習用技術)

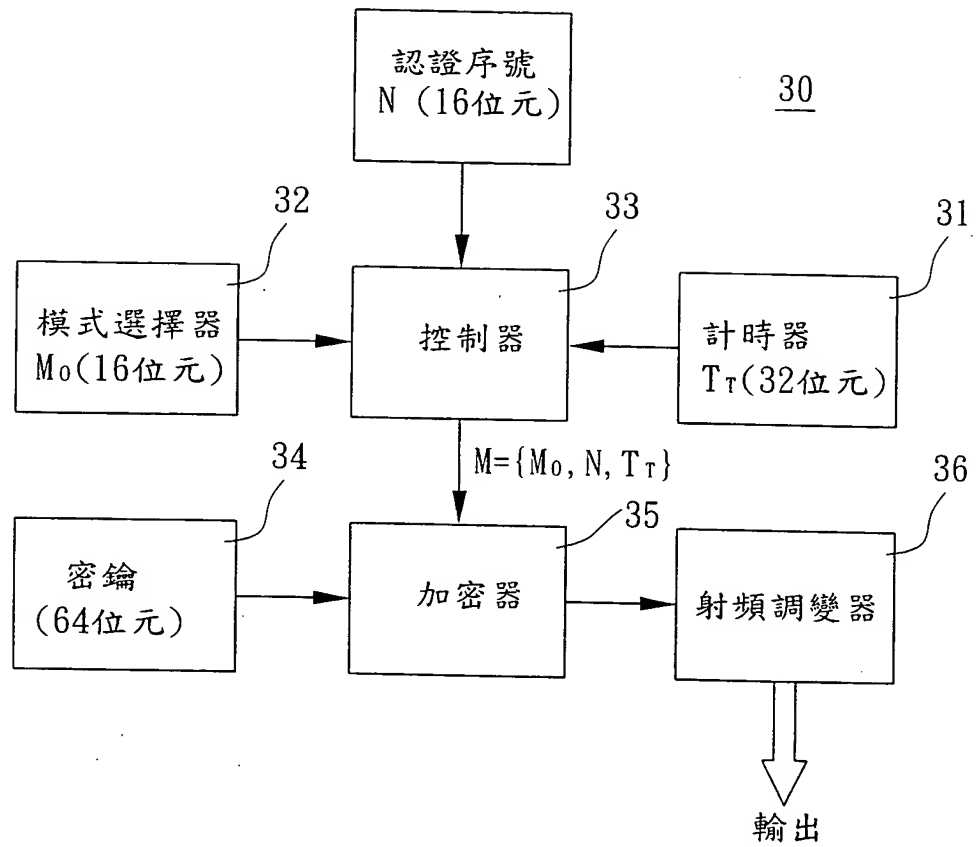


圖 4 A

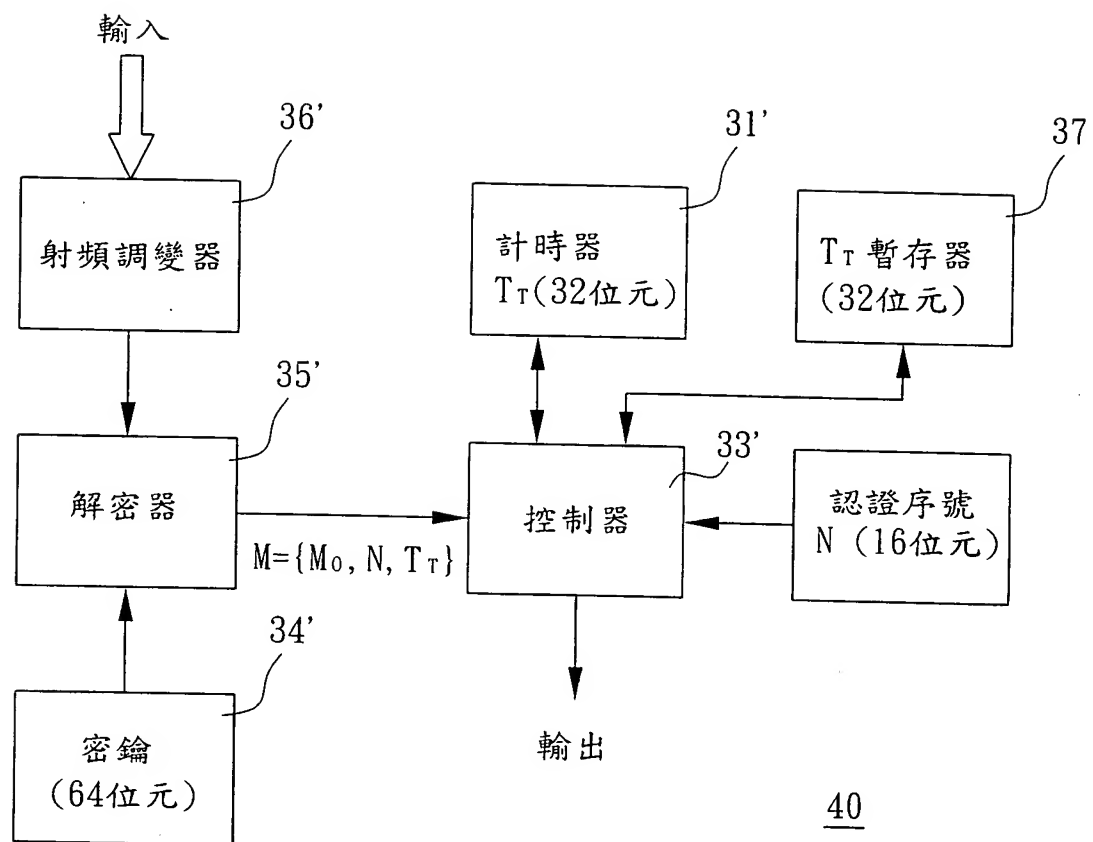


圖 4 B

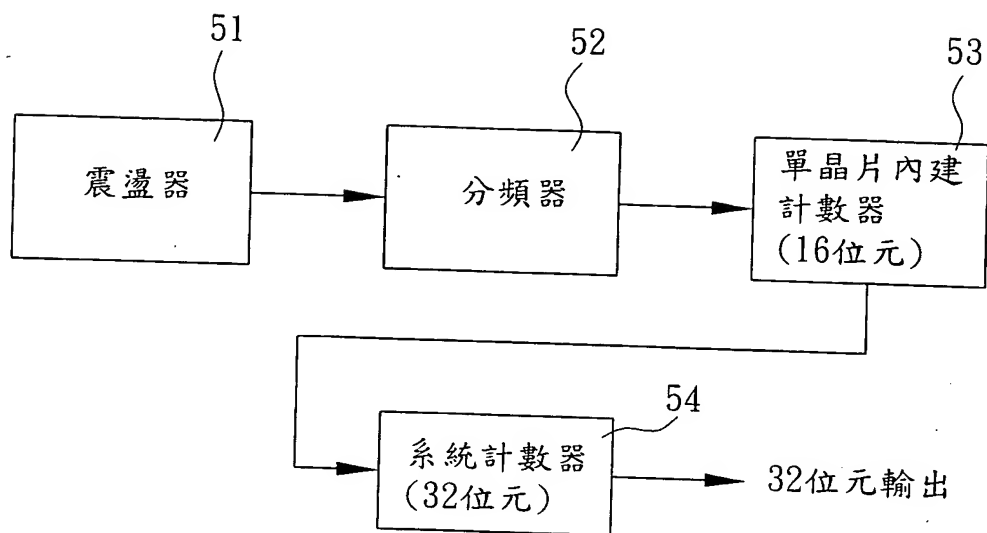


圖 5

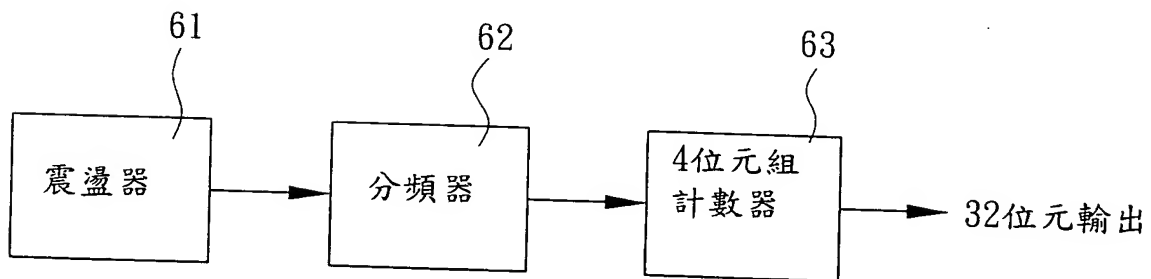


圖 6

容忍/安全時間
與準確度

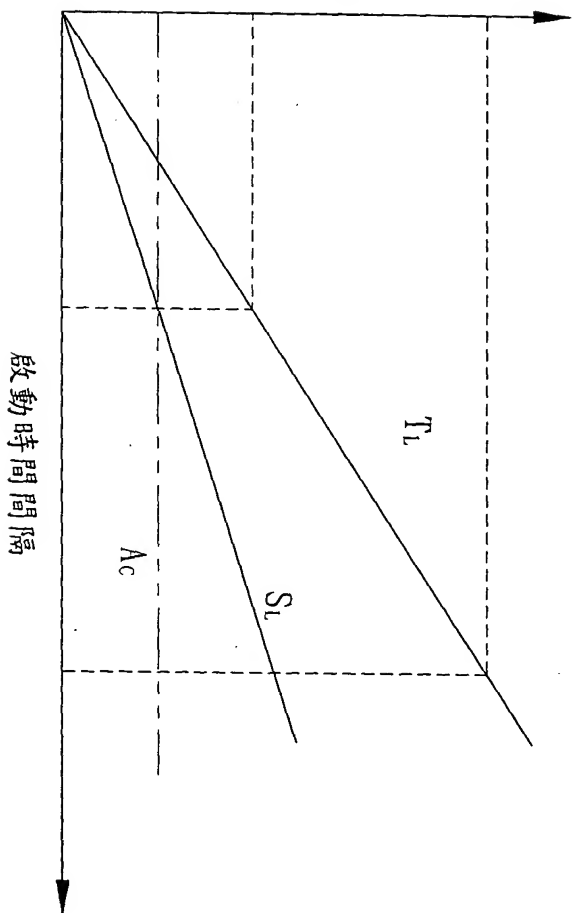


圖 7